P-4-12

New Key Escrow Model for The Lawful Interception in 3GPP*

Kyusuk Han, Chan Yeob Yeun, *Member, IEEE* and Kwangjo Kim, *Member, IEEE*

***Abstract*-- For the lawful interception (LI) of the secure communications, ID-based cryptosystem has the property of key escrow that can be efficiently used for LI. However, it does not prevent the malicious use of the escrowed key by the LEA. Thus, we would like to propose a new key escrow model that enables the limited capability of lawful interception agency.**

I. INTRODUCTION

For the national security or detecting the criminal evidence, the lawful interception (LI) is required in some countries. From the demands of LI, 3GPP provides specifications in [1], [2] and [3].

For the secure communications, a mobile operator has to provide a decryption method for the request of the law enforcement agency (LEA), only if the mobile operator provided the encryption. In general, mobile operators escrow the key of the subscriber and provide the key to the LEA.

The key escrow can be defined as an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that an authorized third party may gain access to those keys under certain circumstances.

In this paper, we would like to apply a new the ID-based cryptosystem (IDBC) that emphasizes the key escrow property. Since the identity of the entity may be used as the key, the IDBC has several benefits of the efficient public key management. However, the IDBC has the problem of re-issuing the secret key from the property that the identity of the entity is used as the key.

Therefore, our motivation is to design a feasible key escrow model based on IDBC in 3GPP for the secure communication that overcomes the shortcoming of key re-issuing. Our novel model shows the efficiency on the public key management. In addition, it doesn't allow the eavesdropping of the LEA that already has the master secret key of the entity for past lawful interception.

II. SHORTCOMINGS OF THE LI

A. LI on the secure communication

The mobile operators have the duty of providing the proper decryption method for the LI of the secure communications under the government regulations, only if they provided the encryption method. For such government regulations, ETSI, ANSI, and 3GPP define the requirements in their specifications.

*This paper was sponsored by Samsung-ICU Center project entitled "Next Generation Mobile Network Platform Security."

B. Key Escrow Models

In the key escrow model, there are two entities: the key escrow agency (KEA) and the law enforcement agency (LEA). KEA escrows the user's keys and offers them to LEA.

After the Clipper became obsolete [4], Abe and Kanda [5] defined the detailed security requirements and the public key cryptosystem based key escrow model that can limit the time bound of interception.

However, above-mentioned model has the shortcoming that the user has to register their secret keys to the KEA. For the requirement of LI, it shows conflict that the users shall not notice that their communications are being monitored.

Thus, we would like to propose a new key escrow model that is based on ID-based cryptosystem (IDBC). IDBC has the key escrow property initially. For the details on the IDBC, please refer [6]. Our security model is based on the mathematical hard problem, as follows.

- **Elliptic Curve Discrete Logarithm Problem**: With given $P, P' \in G_1$, where G_1 is an additive group, find an integer n, which satisfies $P = nP'$.

Since the identity is used as the key in IDBC, the key re-issuing problem happens. Once the LEA knows the key, the LEA is able to know the all information until the key owner re-issues the secret key. However the re-issuing the secret key is only available when the KGC change the master secret.

In the following section, we describe our model in detail.

III. OUR KEY ESCROW MODEL

A. Overview of LI Model

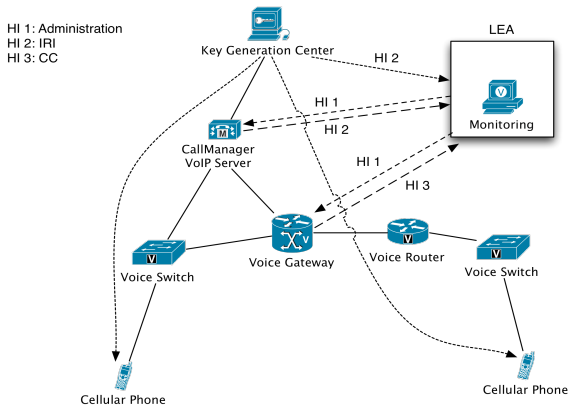

Figure 1 LI Model for the secure communications

We define following entities in our model. The law enforcement agency (LEA) requests a subscriber's communications details to the mobile service provider under the law. The mobile operator (MO) provides the secure

communications service to the subscriber and also provides the communications details to the LEA. The key generation center (KGC) issues the secret key to the subscriber and provides the subscriber's key to the LEA under the law. The subscriber communicates with other subscriber. Fig (1) shows entities in the LI model for the secure communications.

B. Key Escrow and LI Procedures

We assume that two subscribers Alice and Bob communicate each other.

1) Key Generation and Escrow

For the pre-procedure, the KGC operates following.

KGC generates a random integer $s \in Z_P^*$, which will be the master secret of KGC. Each subscriber owns the unique identity ID. KGC generate $sH(ID)$ for each subscriber, where the public knows the hash function $H : Z_P^* \rightarrow G_1$. The multiplication of s and $H(ID)$ is the point multiplication over the elliptic curve. s is stored in the KGC as an escrowed master key.

2) LI Procedures

The LEA requests the KGC and the MO for the lawful interception of the subscriber Alice via HI1. Please refer the section 4.4 in [3] for the detail of HI1, HI2, and HI3.

$Enc_{MO}(r_A \| sign_A(r_A))$

The Symbol $Enc_{MO}(M)$ denotes encryption function, $sign$ is a signature function.

The MO verifies r_A and the signature $sign_A(r_A)$, encrypt them again and send them to Bob.

$Enc_B(r_A \| sign_A(r_A))$

If the MO includes the signature, the MO sends following to Bob.

$Enc_B(r_A \| sign_A(r_A) \| sign_{MO}(r_A \| sign_A(r_A)))$

Bob decrypts the information from the MO, verifies the random number, and generates another random number r_B. After that Bob generate the signature of r_B and sends them to the MO.

$Enc_{MO}(r_B \| sign_B(r_B))$

The MO verifies r_B and the signature, and sends them to Alice. Then, she verifies them.

Alice and Bob compute $devf(r_A, r_B)$, where $devf$ is a function from the input r_A and r_B, implies the general computation including + or ×. The MO also computes $devf(r_A, r_B)$.

The MO sends $devf(r_A, r_B)$ with Alice's ID and the request of lawful interception to the KGC.

The KGC sends $devf(r_A, r_B)sH(ID_A)$ to the LEA via HI2.

The MO sends the interception related information via HI2, and the contents of communication via HI3 to the LEA.

IV. Security Analysis and Comparisons

When the LEA attempts to eavesdrop the secure communications, we assume the two cases. One is that the LEA has no secret key of the subscriber. The other case is that the LEA has the secret key previously used. We consider the former case as the normal adversary, and only focus on the eavesdropping with the secret key that was used in the previous.

In order to eavesdrop, the LEA should be able to know the secret key $devf(r_A^*, r_B^*)sH(ID_A)$ from $devf(r_A, r_B)sH(ID_A)$, where each r_A^* and r_B^* is another random integer from Alice and Bob. Also, the derivation of $sH(ID_A)$ from $devf(r_A, r_B)sH(ID_A)$ is equivalent to computing ECDLP. Thus, it is obvious that our proposed model is secure against the eavesdropping from the LEA.

Table 1 shows the comparisons with previous schemes and our proposed scheme. Our model requires only 1 pre-registered key while Abe-Kanda model requires t+1 keys those are registered by users. Also, our model is applicable to any protocols instead of proprietary protocols. Thus, our model is more efficient than existing previous models.

TABLE I
Comparisons with previous models and proposed model

Property	Clipper [4]	Abe-Kanda [5]	Proposed
Warrant bounds	O	O	O
Admissibility	X	O	O
Fraud detectability	X	O	O
Off-line EA	X	O	O
Sender authentication	?	O	O
Key registration to EA/KGC	Initially registered	O	O
# of secret keys required	1	t+1	1
Key exchange	Diffie-Hellman Key Exchange	Proprietary protocol	Applicable to Any protocols

V. Conclusion

In this paper we proposed the key escrow model for secure communications that is applicable to the lawful interception of 3GPP by using ID based cryptosystem. Our model offers not only the lawful intercepting, but also efficiently prevention of the illegal eavesdropping of the law enforcement agency.

Reference

[1] 3GPP TS 33.106: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements".

[2] 3GPP TS 33.107: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Architecture and Functions".

[3] 3GPP TS 33.108: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; 3G Security; Handover Interface for Lawful Interception (LI).

[4] Clipper Encryption - AT&T Telephone Security Device Model 3600, 2nd, Sep., 1993

[5] Abe, M. and Kanda, M., "A Key Escrow Scheme with Time-Limited Monitoring for One-way Communication", British Computer Society 2002, The Computer Journal, Vol. 45, No. 6, 2002.

[6] Dan Boneh, Matthew K. Franklin, Identity-Based Encryption from the Weil Pairing Advances in Cryptology - Proceedings of CRYPTO 2001